Amendment to the Specification

ApA 9/25/07

In the specification, replace paragraph ~~57~~ 62 with the following paragraph:

As shown in FIG. 4, a user 1 shopping at an online merchant's website, adds items to the online shopping cart. The user chooses to checkout and is provided with the merchant's payment page (STEP 501). The form of the payment page is sent from the merchant's website 210 to the user's browser 11 and includes JavaScript and VBScript to detect the presence of a smart card reader 12. If the reader software is detected, then the user 1 is shown the "Use SCP" option, which invokes the smart card payment (SCP) process (STEP 502). The user 1 selects the "Use SCP" option, which causes the user browser 11 to be directed to the host system 300 user interface 310 (*e.g.*, web server) (STEP 503a) and then to the smart card payment (SCP) system 330 (STEP 503b). The SCP system 330 may include, as appropriate, application servers and databases for processing, storing and managing data. The SCP system 330 saves the user 1 request and redirects the user's browser to an authentication system 320 for appropriate sign-on and authentication (STEPS 504a-d). The authentication system 320, via a suitable sign-on routine, obtains a challenge string from an appropriate user database system 340 (STEP 505). The user 1 is challenged to insert his or her smart card 14 into the smart card reader 12 and enter the appropriate PIN (STEPS 506a-b) – although, as previously noted, any suitable authentication technique is appropriate. In this exemplary embodiment, the user 1 enters the PIN, resulting in the challenge string being signed and returned, with a digital certificate, to the host system authentication system 320 (STEP 507a-b). The digital certificate and the signed challenge string is passed to the user database system 340 where the user 1 is identified from within various user and/or account information database tables (STEP 508). The user may thus be authenticated by comparing the digital certificate to the signed challenged string or by comparing either the digital certificate or the signed challenged string to a third data set stored in the user and/or account information database tables. It should be appreciated that the data structure may be configured in any number of suitable ways, comprising a plurality of servers and databases as desired. The authentication system 320 signs the user a into the host system's security system 350 that facilitates the secure exchange of data between servers and databases (STEP 509).

Serial No. 09/943,658
Docket No. 40655.4400

Amendment to the Specification

MYA
9/25/07

In the specification, please replace paragraph 59 ~~54~~ with the following amended paragraph:

FIG. 2b illustrates an alternative embodiment, where the merchant 200 system is configured to maintain active control of the user 1 browser during the authentication and STN generation process. This may be desired by some merchants who do not want to send a user 1 to a host system 300 out of concern, for example, that they may loose that valued consumer. The merchant 200 system in this embodiment is configured to act as a throughput of information between the user 1 and the host system 300. As depicted in FIG. 2b, the user 1 selects products or services to purchase from a merchant website 210 (STEP 401). The merchant 200 detects the smart card reader 12 on the user 1 device 10 and displays the smart card button 218 (STEP 422). The user 1 then chooses to use the smart card payment system by selecting the smart card button 218 (STEP 423). The Merchant 200 calls the host system 300 using a secure and authenticated channel (*e.g.*, SSL) to retrieve a challenge (*e.g.*, to insert card and enter PIN) from the host system (STEP 424). This challenge is passed along to the user 1 (STEP 425) within a merchant authentication web page 320. The user 1 inserts the smart card 14 and enters the proper PIN in the appropriate authentication field 321 (STEP 426). A signed challenge string and a digital certificate are ~~is~~ passed to the merchant 200 and on to the host system (STEP 427). The host system 300 authenticates the user 1, identifies the user's account information, and if more than one user account is available, provides the user the ability to select from multiple accounts on the merchant's account selection page 322. For example, the user 1 may be presented with a list of the last four digits of the available account numbers. A STN is generated and associated with the selected user 1 account in a host system 300 STN database. During settlement, the actual user 1 account number is resubstituted for the STN and processed for payment and invoicing. The STN is provided (along with other transaction data if desired) directly to the merchant 200 (STEP 428). The initial transaction is completed when the merchant 200 accepts the secondary transaction number (and other transaction data) from the host system 300 and notifies the user 1 (STEP 429).